JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Cyber AI

Cyber-Augmented Operations Technical Symposium

March 2019

Elisha Peterson
elisha.peterson@jhuapl.edu
Chief Scientist & Lead for Cyber AI, Analytic Capabilities Group
Johns Hopkins University Applied Physics Laboratory

Summary

- How do we leverage AI/ML (and visualization) to make operators more effective

Effective Analytics

Ask the Right Questions

↓

Use the Right Data

↓

Apply the Right Tools/Techniques

↓

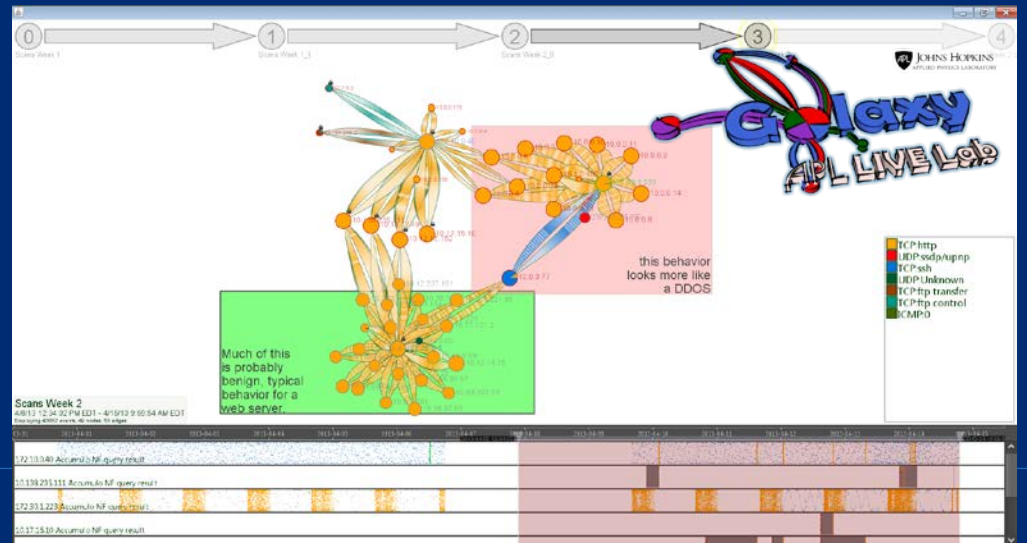
Apply Answers to the Right Situation

↓

Ensure Value to Operators

Ask the Right Questions

- Visualize data to better understand context, find new anomalies
- Train data scientists in cyber, e.g. by embedding with operators/exercises/etc.
- Be more specific
  - *Not “what netflow is malicious” but “when do these clients open an unusual port?”*
- Be more comprehensive
  - *Not “do any bad hosts talk to my web server?” but “what are the set of all allowed/expected flows for this web server?”*

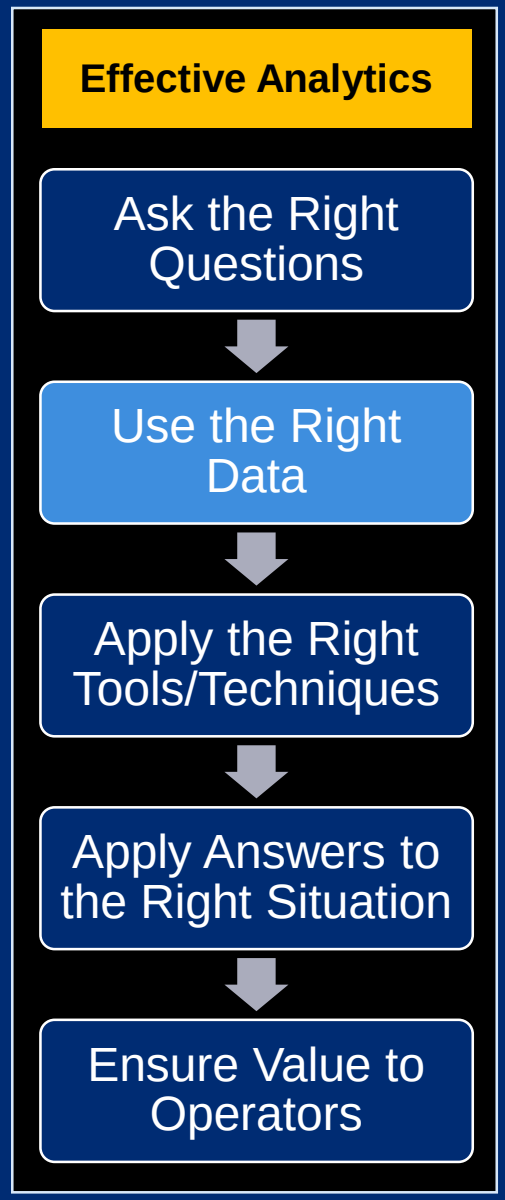


Effective Analytics

1. Ask the Right Questions
2. Use the Right Data
3. Apply the Right Tools/Techniques
4. Apply Answers to the Right Situation
5. Ensure Value to Operators

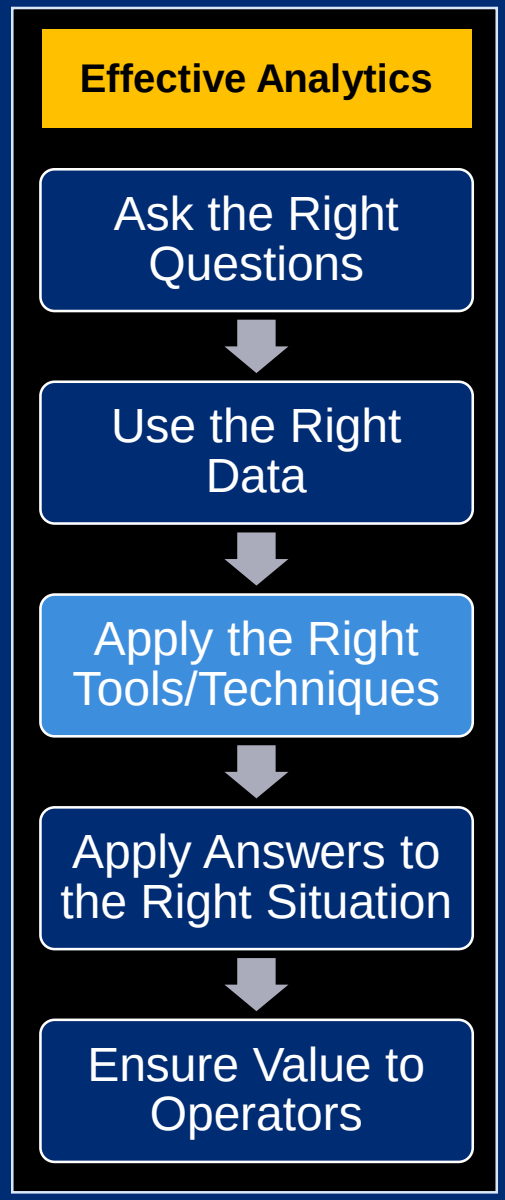
Use the Right Data

- Need good labeled data
  - 1999 DARPA Intrusion dataset – flawed, out of date, dozens of papers
- Need more than just netflow
  - Collect from multiple locations for cross-site correlation
  - Collect from multiple types for corroboration/ground truth
- Repeatable experimentation platforms?



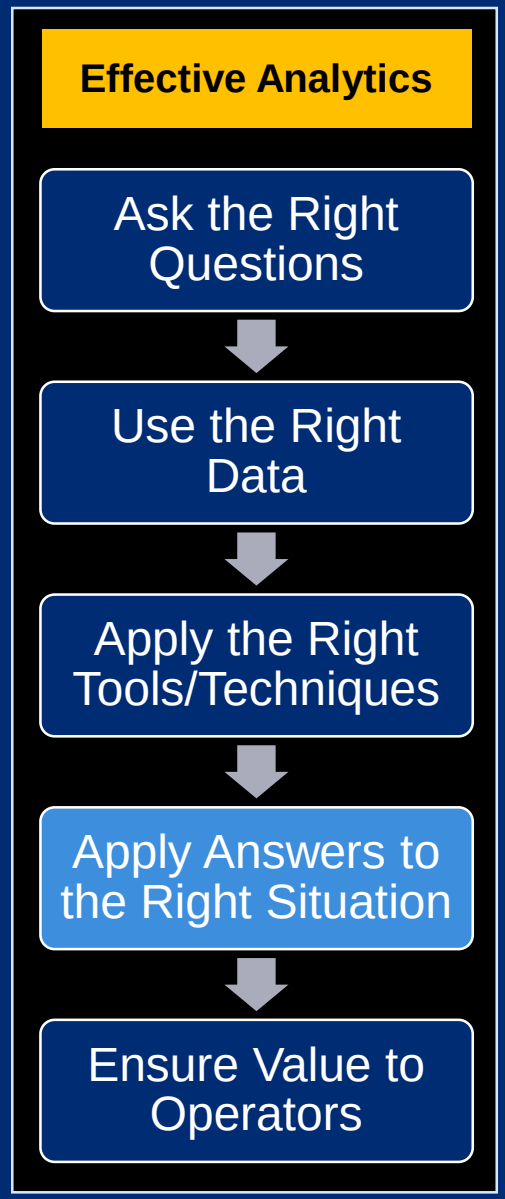
Apply the Right Tools/Techniques

- What is the simplest technique that will work?
- Techniques that work well in one domain may not work well with cyber
  - Deep learning is not “one size fits all”
- Feature Engineering / Domain Understanding
  - Add statistics for packet sizes/times within a flow
  - Model connections between (ip+proto+port) rather than ip’s
- Incorporate modeling, e.g. attack graphs



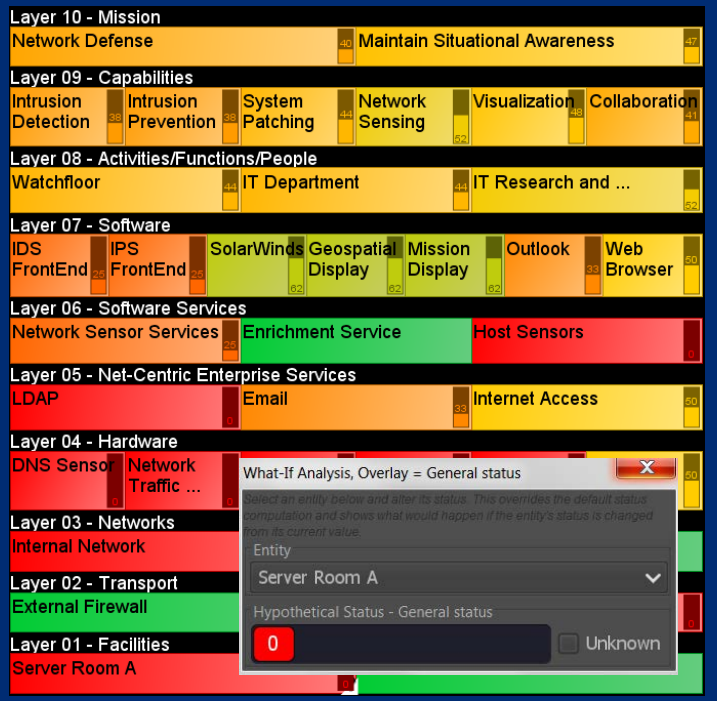
Apply Answers to the Right Situation

- Context matters: enterprise networks, research networks, university networks, ICS/SCADA networks, other constrained networks
- Need more research on transferability of models



Ensure Value to Operators (Users)

- Who is the user?
  - *analyst? defensive/offensive ops? decision-maker? developer? data scientist?*
- Analysts
  - Need low false positives
  - Need context, especially with alerts
- Decision-makers
  - Tools like Dagger can help decision-makers understand impact and prioritize resources
- Data scientists
  - AI to make analytic development faster?



Effective Analytics

Ask the Right Questions

↓

Use the Right Data

↓

Apply the Right Tools/Techniques

↓

Apply Answers to the Right Situation

↓

Ensure Value to Operators

Application Areas Where AI Is Likely to Help

- **Anomaly Detection**
- **Cyber Key Terrain Mapping**
- **Automated Data Science**
- **Planning & Executing Cyber Ops**

- **Currently helping** – malware analysis, spam detection, DNS queries, …

Challenge #1: Establish Cyber CTF

- Common Task Framework
  - Requires **public** data sets, automated evaluation/metrics, and a competition
  - Establishes feedback loop for constantly improving models and techniques
  - Always leads to declining error rates
- What would a CTF for cyber look like?
  - Define classes based on both host roles (web, DNS, enterprise client, etc.) and traffic (web, scanning, video, data exfiltration, etc.)
  - Models must grapple with cyber semantics to be successful
  - Goal becomes “out of all this traffic, what is understood and what is not understood”

Challenge #2: Automated Network Characterization

- From an observed set of data, define the rules that govern that data
  - Subnets, firewalls, servers, applications, etc.
- Difficulty varies by network type: constrained, enterprise, research
- Immediate value for alerting on constrained networks
- Immediate value for CPTs understanding an unfamiliar environment

**also known as "key cyber terrain mapping"*

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY

Application Areas Where AI Is Likely to Help

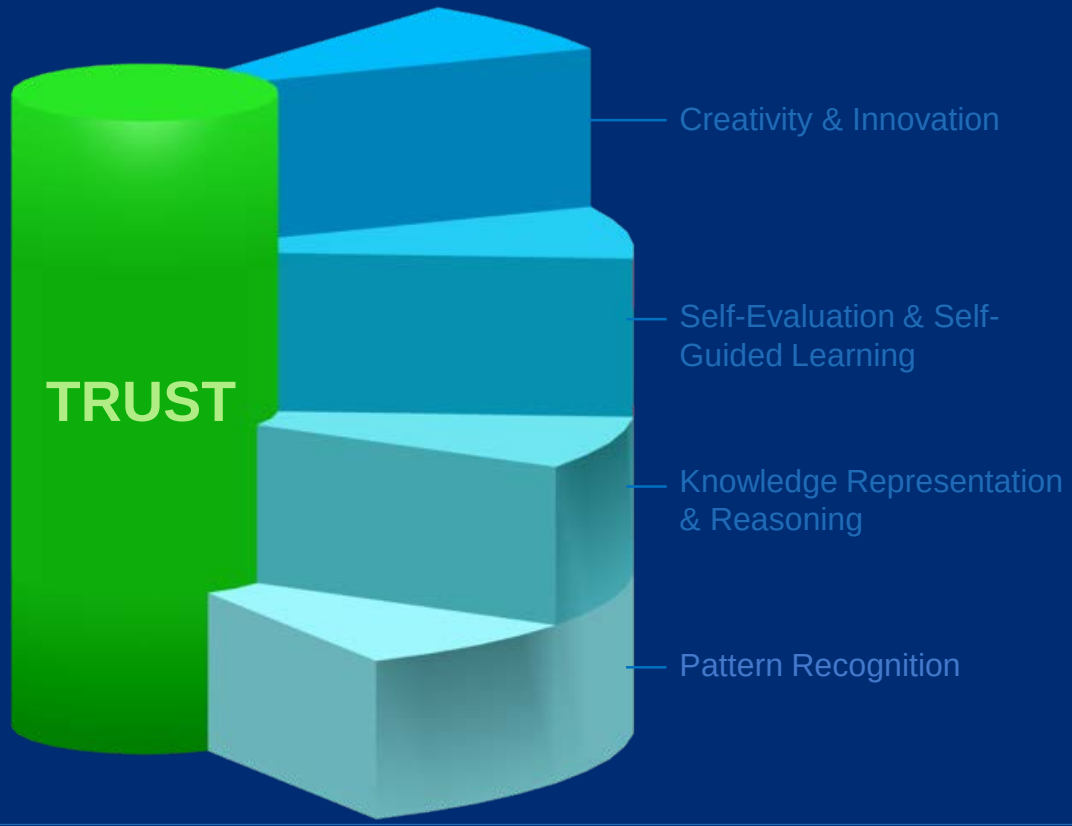
- **Anomaly Detection** – finding unknowns, combinations of techniques, zero days
  - Likely adds less value for known attacks when strong signatures are available
- **Analytic Assistance** – automated enrichment, query expansion, information aggregation, correlation
- **Cyber Key Terrain Mapping** – automated network discovery, mapping to mission
- **Automated Data Science** – developing, testing, deploying, maintaining ML and other analytics models in production; enabling end-users to harness the power of ML
- **Planning & Executing Cyber Ops** – human/machine teaming for planning, analysis, COA selection, rapid employment of defenses and effects in cyberspace

- **Currently helping** – malware analysis, spam detection, DNS queries, …

Intelligent Sensing Vision

Autonomously understand the world as a trusted partner to the symbiosis of humans and other AIs

Perceive • Decide • Act • Team



Reasoning

Ability to deal with the unexpected